REMARKS

Claims 1-20, 22-24, and 26-32 remain pending. Claims 21 and 25 are cancelled. Applicants have amended claims 1, 23, 27, and 29 to clarify that the user is connected to the network through an access server and that an authorization parameter is used by the access server to grant or deny access. Applicants have also amended claims 19 and 20 to correct typographical errors.

Summary of the Office Action

The Office Action rejects claims 1-4, 6, 11-14, 16-19, 21-29, and 31 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,182,142 ("Win"). The Office Action rejects claims 5, 9, 10, and 15 under 35 U.S.C. § 103 as unpatentable over Win in view of U.S. Patent No. 6,493,749 ("Paxhia"). The Office Action further rejects claims 7, 8, 20, 30, 32 under 35 U.S.C. § 103(a) in view of Official Notice.

Discussion of the Rejections under 35 U.S.C. § 102

The Office Action rejects claims 1-4, 6, 11-14, 16-19, 21-29, and 31 under § 102 as anticipated by Win. Claim 21 is cancelled. Accordingly, the rejections under § 102 remain with respect to claims 1-4, 6, 11-14, 16-19, 22-24, 26-29, and 31. Applicants submit that the pending claims are patentable over Win for the reasons discussed below. Accordingly, withdrawal of the rejections and reconsideration are respectfully requested.

1. Claims 1-4, 6, 23, 27, 29

Independent claims 1, 23, 27, and 29 are directed to a method and system for granting and denying a request by a user or computer to access a resource on a network. As amended, each of these claims recite a configuration wherein the user is coupled to the network "through a network access server, the network access server being interposed between the user and the resource." In response to an attempt by the user to access a resource on the network, a group to which the user belongs is determined. Based on the determined group, "an authorization parameter" is selected and the authorization parameter is used "by the network access server" to grant or deny access to the resource.

Win discloses a network wherein a user (browser 100) is directly coupled to a network 102 that includes protected resources 208 located on protected servers 104, 112. (FIGs. 1 and 4).

An access server 106 is also directly coupled to the network. (FIG. 1). When the user first attempts to access the network, the user is prompted to enter a user name and password. An authentication client module 414 in the access server authenticates the user by name and password and then, if the authentication is successful, embeds an encrypted user cookie and a roles cookie into the browser 100. (FIG. 4; col. 6, ll. 48-61; col. 8, ll. 31-67). When the user attempts to access a particular resource by opening a URL, the browser 100 sends the cookies to the protected server having the protected resource to which access is desired. (col. 6, l. 65 – col. 7, l. 5). The protected server with the protected resource then examines the encrypted information in the user and roles cookies to determine whether the user should be permitted access. If the user is not permitted to access the protected resource, a runtime module 206 in the protected server 206 redirects the user to a predefined URL. (col. 8, l. 56 – col. 9, l. 5).

Win does not anticipate amended independent claims 1, 23, 27, and 29 for at least two reasons. First, each of these claims recite a network configuration wherein the user is coupled to the network through the network access server and wherein the network access server is interposed between the user and the resource. As discussed above, Win discloses that the user (browser 100) and access server are both directly connected to the network. Thus, and in contrast to the claimed invention, the access server disclosed in Win is not interposed between the user and the network.

Second, claims 1, 23, 27, and 29 recite that the authorization parameter is used by the network access server to grant or deny access. Win discloses an access server, however, the access server in Win does not grant or deny access to network resources. Instead, the access server disclosed in Win embeds cookies into the user's machine. Win further discloses that the user communicates directly with the protected server having the desired resource. During that direct communication, the user sends the user cookie and roles cookie to the protected server. The protected server then grants or denies access based on the information in the cookies. Thus, the method and system disclosed in Win requires that each individual server with the protected resource determine whether to grant or deny access. In contrast, the claimed invention provides a method and system where the decision to grant or deny access is made by a central network access server thereby obviating the need to implement the software on each and every machine with a resource to be protected.

Because Win fails to disclose, teach, or even suggest a method or system wherein a user is coupled to the network through a network access server or wherein an authorization parameter

is used by the network access server to grant or deny access to a resource, Win does not anticipate independent claims 1, 23, 27 and 29.

Claims 2-4 and 6 depend from claim 1 and are patentable for at least the same reasons. Additionally, claim 2 recites determining "a characteristic of the link, and selecting the authorization parameter based on the determined characteristic." Thus, in claim 2, the selected authorization parameter is based on characteristics of the link over which the user attempts to access the resource. The Office Action indicates that this feature is disclosed in Win at col. 6, lines 48-61. However, the portion of Win relied upon by the Office Action describes a process wherein encrypted cookies are sent from the access server to the browser 100. Win does not disclose that the link between the user and the access server is examined to determine a characteristic, and further does not disclose selecting an authorization parameter based upon the determined characteristic. Thus, claim 2 is not anticipated by Win for this additional reason.

2. Claims 11-14, 16-19, 22, 24, 26, and 28

Independent claims 11, 22, 24, 26, and 28 are directed to configuring a data path through which a user or computer is connected to a network. A group to which the user belongs is determined. Based upon the determined group, a "communication parameter" is selected and the communication parameter is then used to "configure a data path" between the computer and the network in accordance with a policy.

According to the Office Action, "Win discloses selecting a communication parameter wherein the communication parameter is usable to configure a data path between the computer and the network in accordance with the policy in (col. 5, lines 5-15). Data path and IP address for the data path is disclosed in (fig. 9 and col. 9, lines 53-62)." To the extent this suggests that Win discloses selecting a communication parameter based upon a determined group and then using the communication parameter to configure a data path as claimed, Applicants respectfully disagree.

As discussed above, Win discloses a particular method of granting or denying access to a resource on a protected server based on a roles cookie and a user cookie sent from a user to the protected server. There is a distinction between "communication parameters" (as recited in claims 11, 22, 24, 26, and 28) and the roles and user cookies disclosed in Win. As claimed, and as discussed in Applicants' specification, communication parameters are used to configure the data path (e.g. set characteristics such as bandwidth, speed, IP address, media, protocols used, and the like). (pages 9-10). In contrast, the roles and user cookies in Win are used to determine

whether to grant or deny access to a particular network resource. Win does not disclose, teach, or even suggest that the roles and user cookies are used to configure the data path as claimed.

Applicants agree with the indication in the Office Action that a data path and an IP address for a data path are generally disclosed in Win. However, such disclosure in not sufficient to anticipate the rejected claims because the claims do not simply recite a data path and an IP address. The rejected claims more specifically recite configuring the data path based upon communication parameters that are selected based upon a user's determined group, which for the reasons previously discussed is simply not disclosed in Win. Accordingly, independent claims 11, 22, 24, 26, 28 are patentable over Win. Claims 12-14 and 16-19 depend from claim 11 and are patentable for at least the same reason.

3. Claim 31

Claim 31 recites determining a medium type of a communication medium through which a user attempts to access a network and determining a group to which the user belongs. The determined group and medium type are then used to determine whether to grant or deny access. As previously discussed, Win discloses that roles cookies and user cookies are used by a protected resource to grant or deny access. Win does not disclose, teach, or even suggest determining a medium type or basing a decision on whether to grant or deny access based upon the medium type. Accordingly, claim 31 is not anticipated by Win.

Discussion of the Rejections Under 35 U.S.C. § 103

The Office Action rejects claims 5, 9, and 10 under § 103 as unpatentable over Win in View of Paxhia. Claims 5, 9, and 10 depend from claim 1. As previously discussed, Win does not disclose, teach, or even suggest that the user is coupled to the network through a network access server, or that the network access server uses an authorization parameter to deny or grant access to the user as recited in claims 5, 9, and 10. Paxhia is relied upon for its disclosure of override attributes. However, Paxhia likewise fails to disclose, teach, or even suggest placing an access server between the user and network and using the access server to grant or deny access. Accordingly, Paxhia and Win do not disclose, teach, or suggest the invention as recited in claims 5, 9, and 10.

Finally, the Office Action rejects claims 7-8, 20, 30, and 32, over Win in view of Office Notice. Claims 7-8 are directed to a method wherein a user is coupled to a network through an access server and the access server grants or denies access to a resource on the network based on

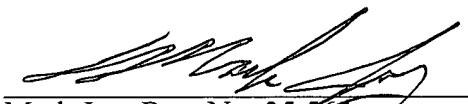
a determined group. Claims 20, 30, and 32 are directed to selecting a communication parameter based on a determined group and using the communication parameter to configure a data path. For all of the reasons previously discussed herein, Win fails to teach using an access server to grant or deny access or a method or system for configuring a data path based upon a determined group. Accordingly, claims 7-8, 20, 30, and 32 are patentable over Win in view of the Official Notice.

If the rejections are maintained in a subsequent Office Action in view of Official Notice, Applicants respectfully request a reference teaching the features that are not disclosed in Win.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,



Mark Joy, Reg. No. 35,562
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: September 25, 2003